AUTOMATED TELLER MACHINE USING UMP SMART CARD IN DB2

WONG KAM MAN

A thesis submitted in partially fulfillment of the requirements for the award of degree of Bachelor of Computer Science (Computer System and Networking)

Faculty of Computer System & Software Engineering

Universiti Malaysia Pahang (UMP)

JUNE 2012

ABSTRACT

This document discusses about Automated Teller Machine using UMP smart card in DB2. In UMP, students, lecturer, or staff might bring more than one smart card with them and thus there is always make inconvenient for them. This project is developed to use an all-in-one smart card that can perform banking transaction and perform as student ID card or staff ID card as well. The proposed system will have two part, user interface and database. The database is installed in z/OS environment while the user interface is in Windows. To develop this proposed system, System Development Life Cycle (SDLC) has been chosen as methodology.

ABSTRAK

Dokumen ini bincang tentang *"Automated Teller Machine using UMP smart card in DB2"*. Di UMP, mahasiswa, lecturer and kerani mungkin membawa lebih daripada satu smart card dan inilah sentiasa menyebabkan kesusahan. Projek ini dibangunkan untuk penggunaan all-in-one smart card yang boleh melaksanakan transaksi perbankan dan digunakan sebagai matrik kad mahasiswa atau matrik kad kerani. Sistem yang dicadangkan dibahagi kepada dua bahagian iaitu user interface dan database. Database install di dalam persekitaran z/OS manakala user interface install di dalam Windows. Untuk membangunkan system yang dicadang ini, System Development Life Cycle (SDLC) telah dipilih sebagai metodologi.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

This chapter briefly describes the Automated Teller Machine using UMP smart card in DB2. This chapter comprises five sections which are the background of the project, problem statements of the project, objectives and scope of the project.

1.1 Background of Proposed Study

The system that will be developed is Automated Teller Machine using Universiti Malaysia Pahang (UMP) smart card in DB2. It is a system where a multi-function smart card will be used on an ATM instead of using a normal smart card. Also, the system will use z/OS mainframe as the backbone core server to control the ATM system.

Automated Teller Machine (ATM) is actually a computer that is connected on a twenty-four hours real-time system to let end users perform banking transactions, make inquiries concerning the status of their accounts, pay bills and obtain other banking services in a public place. To use the ATM, each user needs to have his/her own ATM card that contains a PIN number to access their accounts.

Operating systems such as Windows or Linux are not sufficient to maximize the performance of the mainframe. The most suitable operating system for mainframe is

z/OS designed by IBM. Mainframe, famous for its heavy workload performance, is suitable for the backbone of Automated Teller Machine.

In UMP, everyone needs a matric card as the passport to enter the administrative offices, lecture halls, labs, and library. The matric card has no other functions except as mentioned above. These also implied on our Identity Card (IC). Our IC doesn't have any functions although it is a smart card which contains a chip on it.

1.2 Problem Statements

For the current system, end users need to bring a specific ATM card for a specific ATM, so the end user might end up having a lot of cards. Current smart cards such as Identity Cards (IC) or Student Cards have no any function. It is kind of a waste as they do not serve any purpose.

1.3 Research Objectives

The objectives of the proposed system are listed as the following:

1.3.1 To implement an all-in-on ATM card system that can be used to withdraw cash and check inquiries.

1.3.2 To make it convenient for end users so that they do not need to bring more than one card.

1.4 Scope of Study

The users of the proposed system are UMP students, staff and lecturers. UMP students, staffs and lecturers withdraw cash from ATM, use the top-up service ATM provide, e-payment, and use their smart card to enter administrative offices such as JHEPA, faculties, lecture halls and labs, and the library. There are some limitations as the proposed system equipped with cash withdrawal and check balance inquiry functions however just for testing purposes only.

CHAPTER 2

LITERATURE REVIEW

This chapter briefly describes the reviews on existing techniques related with Automated Teller Machine using UMP smart card on z/OS environment that will be developed later. This chapter comprises of history of Automated Teller Machine, Security of ATM, Cost issue of ATM, Types of Smart Card, Security of Smart Card, Advantages and Opportunities, Databases and Computers.

2.1 History of Automated Teller Machine (ATM)

As said by Bernardo Batiz-Lazo and Robert J.K. Reid (2011), Cash dispensers or Automated Teller Machine (ATM) in the United Kingdom emerged independently and in parallel with similar technologies in Japan, Sweden, and the United States. The Committee of London Clearing Banks (CLCB) formed an Electronics Subcommittee, which had a mandate to research possibilities of brining electronic computing to British banking and was pivotal in establishing the banks that would become early computer pioneers in 1955. Barclays Bank, Britain's biggest in terms of deposits, opened the first

dedicated center to house a mainframe computer in 1961. Soon, the first ATM was introduced at Barclays Banks in Enfield, United Kingdom in June 1967.

On most modem ATMs, the customer needs to insert a plastic ATM card with a chip or a magnetic strip that contains a unique card number and some security information such as a PIN number to access his/her banking account. ATM security is one of the issues that cause concern.

2.2 ATM Security issues

Security of ATM is an issue that always concerned by people. After we put in our card into the ATM, we are prompted to input a PIN before the cash withdrawal is procedure. As Coventry L., Angeli A. D. and Johnson G. (2003) mentioned, many people have PINs and password for a multitude of devices, from car radio and mobile phone, to the computer, web-based services and their bank information. Soon Kim C. and Mun-Kyu L. (2010) also noted that Personal identification number (PIN) is a common method to authenticate a user for various devices including ATMs, mobile phones, PDAs, door locks and so on. Normally we will choose to our own password or PINs for those devices. Coventry L. et al. (2008) stated that if people are permitted to choose their own passwords they tend to use the one which are easily guessed. Normally the passwords that people choose are related to their everyday life. The passwords are easy to remember, easily predicted, or some people might change all PINs to be the same. Moncur W. and Leplatre G. (2007) also said that PINs are easily forgotten and users circumvent the forgetfulness by write down theirs PINs, make the PINs all the same, or disclose them to friends and family. This make the PINs security is weak. Munjal N. and Moona R. (2009) noted that a fake outlet can acquire user's details from their magnetic card and even take their PIN without dispensing services. Soon Kim C. and Mun-Kyu L. (2010) stated that if someone observes the input procedure by looking over a user's shoulder or using a tiny camera, he can easily obtain the PIN. This kind of attack is called 'Shoulder surfing attack (SSA). According to Mohammed A.M.

Abdullah, F.H.A. Al-Dulaimi, Waleed Al-Nuaimy and Ali Al-Ataby (2011), a user gains access to a card if he/she enters the right PIN. These shown that our PINs or private information might be obtained by attacker. Also, attacker might withdraw money from the victim's account after getting the PINs.

It is very clear that, awareness is needed. Moncur W. and Leplatre G. (2007) stated that awareness is emerging of the need to design authentication with usability. There are many options to design the authentication, include biometrics, personalization and behavior, and graphical passwords. Coventry L. et al. (2008) noted that biometric techniques can confirm that a person is actually present without requiring the user to remember anything. While Moncur W. and Leplatre G. (2007) mentioned that graphical passwords offer greater usability, potentially greater security than knowledge-based passwords. Soon Kim C. and Mun-Kyu L. (2010) defined certain security aspects which are complexity of a random guessing attack, Resilience to human shoulder surfer, and Resilience to recording attack. Complexity of a random guessing attack is the number of choices an attacker faces when he tries to pass the PIN entry test by a random guessing attack. Resilience to human shoulder surfer is the amount of information that a human attacker without any recording device must memorize to recover PIN. Resilience to recording attack is the size of a set for PIN candidates consistent with the current transaction when the whole procedure is recorded by a camera. Munjal N. and Moona R. (2009) said that two levels of authentication, first using Public Key Infrastructure (PKI) based authentication and second using biometric trait like a fingerprint. They believe that this scheme prevents card forgery and phishing attacks. Cooke J.C. and Brewster R.L. (1993) mentioned that the security requirements in personal communication system are twofold; they are authentication and protection of information.

2.3 Cost Issues of ATM

Another issue of current ATM is cost issue. As mentioned by Munjal N. and Moona R. (2009), Network connectivity is indispensable to the working of the current

transaction model. Hence, the network component contributes heftily to the run time costs of the model. They also noted that unreliable network as another issues of ATM. Financial services that use the network, claim round the clock availability. Dedicated network connectivity is a possible downfall of the current model not only because it is difficult to achieve in distanced rural areas but also because networks are said to be inherently unreliable. Lastly, Burden of carrying multiple tokens is one of the critical issues of ATM. Users often carry multiple authentication tokens such as a magnetic stripe card, smart card, RF card etc. for multiple services like credit account, debit account etc. and for each of the subscribed financial institution and cause a lot of overhead for the users.

2.4 Types of Smart Card

Attoh-Okine N. O. and David Shen L. (1995) specified two types of smart cards, the contact-type or the contactless type while Katherine M. S. and J. Drew Procaccino (2002) categorized the smart card as either a memory card or a processing-enabled card. Both statements are actually correct. A smart card can either be a memory card or a processing-enabled card, as well as either contact type or contact-less type. Contact card requires physical contact between the card and the reader while contactless card is either close-range or long-range, reliable and more expensive compared to a contact card. According to Katherine M. S. and J. Drew Procaccino (2002), the simplest form of smart card is memory card, with limited capability to securely store personal information. Next is prepaid card, which transfer the electronic equivalent of cash to a vendor's digital cash register. The processor-enabled smart card is which based on semiconductor technology with a smart chip with few hundred bytes of RAM. The memory capacity of processor-enabled smart card to function as a multi application card, combining many functions such as credit card, debit card, stored value card, information management card, and loyalty card. They also mention that smart card has nonvolatile, read-only memory (ROM), random access memory (RAM) and central processing unit (CPU). Arafatur

Rahman et al. (2008) also state that smart card have electrical contacts and a thin metallic plate, which is an integrated circuit chip (IC) that containing a central processing unit (CPU), random access memory (RAM) and non-volatile data storage. Also, Schaefer R., Mueller W., Lopez A. M. and Sanchez D. D. (2007) state that the common of SIM cards for mobile phones, credit card sized contact or contactless cards, and card in USB connectors is their limited processing power and data storage.

Similarly with the current ATM system, the smart card that will be used in my proposed system is the contact type smart card which is a memory card that can store banking account ID, PIN number and some personal information such as name and Identity Card number.

Feature Component	Smart Card	
	Memory Card	Processor-Enable Card
Read Only Memory?	yes	yes
Random Access Memory?	no	yes
Microprocessor?	no	yes
Contact/Contactless Interface	contact, contactless or both	contact, contactless or both
Data certified secure (ITSEC*)?	no	yes
Example	phone card	multi-application cards

* information Technology Security Evaluation Certification represents a set of software and hardware security standards that have been adopted in Europe and Australia.

Figure 2.1 Memory Card versus Processor-Enable Card

2.5 Security of Smart Card

Basically, security of smart card can be categorized in authentication, authorization and transaction processing. As mentioned by Katherine M.S. and J.Drew Procaccino (2002), there are three categories of smart card applications which are authentication, authorization, and transaction processing. The security requirement of smart cards is authentication and protection of information (Cooke J.C. and Brewster

R.L., 1993). Attoh-Okine N.O. and David Shen L. (1995) also discussed the security requirement of smart cards in terms of account verification, user identity verification, information access restriction and prevention of card attemping. Financial service outlets need authentication, integrity, confidentiality, non-replication and non-repudiation (Munjal N. and Moona R., 2009).

We can conclude that the security of smart card mainly focus on authentication, protection of personal information and also information access restriction. ATM system needs very strong security to protect the user and banking transactions. Therefore, security of smart card needs to be frequently upgraded to always protect and secure each transaction and user information.

In my proposed system, to recognize users, we need to enter a correct PIN number which matches the PIN number stored inside the smart card. If the PIN number entered is wrong at most three times, the card will be temporarily blocked by the system and no banking transaction is allowed with the card.

2.6 Advantages and Opportunities

By using the smart card, Attoh-Okine and David Shen L. (1995) said that the flexibility of a system's structure, accountability and security and convenience for users might be improved. As mentioned by Katherine M. S. and J. Drew Procaccino (2002), new traffic offences could be updated to a person's smart card within minutes of the offense. The smart card also has the potential to facilitate storage of demographic information for voting purposes. This is clear that by using the smart card, the effectiveness of the system would be improved. Using smart card benefits to the security of personal communication systems (Cooke J.C. and Brewster R.L., 1993) which means, the smart card improves the security of the systems as mentioned by Attoh-Okine and David Shen L. (1995).

2.7 Database

Database in mainframe is using DB2 while normal server using MySQL or Oracle as the database. Here, the different between DB2, MySQL and Oracle will be reviewed regarding the security, price, features, availability of platform, backup and recovery, and storage.

2.7.1 Security

Database such as Oracle or MySQL is normally used in Windows or UNIX system while DB2 is specially designed for z/OS mainframe. According to Trivedi G. (2010), Oracle server has a Database Management System (DBMS) that controls the stocking of data, recovering of data through adequate optimization techniques, security of the databases and tasks allowed for particular users and consistency and protection of data, including task archiving and search engines. While MySQL uses three parameters to authenticate a user namely user name, password and location, Oracle uses so many security features like username, password, profile, local authentication, external authentication, advance security enhancement and etc. (Shekhar R., 2011) Ebbers M. et al. (2009) noted that DBMS in z/OS is able to put confidential or sensitive data in a separate segment or table while in a Partitioned Data Set (PDS) or Visual Storage Access Method (VSAM) flat file, the application program gets access to every data element in the logical record.

2.7.2 Price

When we want to choose a suitable database server, price is one of a factor affects our decision. Trivedi G. (2010) mentioned that Oracle is more costly than DB2 although Object wise comparison is same in both RDBMS which mean triggers, functions, tables, bitmap indexes, tree indexes, PL/SQL and etc are in same in both Oracle server and DB2. On the other hand, MySQL is an open source database, and is completely free. (Shekhar R., 2011).

2.7.3 Features

According to Trivedi G. (2010), IBM DB2 UDB was specially created to support features of Business Intelligence directly in the database. These abilities include data mining, ETL, OLAP and other advance space features of analysis and statistics. Shekhar R. (2011) noted that MySQL database does not support any feature like Audit Vault on its server while Oracle, supports several extensions and programs on its database server for instance, Active Data Guard, Audit vault, Partitioning and Data Mining.

2.7.4 Availability of Platform

According to Trivedi G. (2010), Oracle server is almost available for every operating system like Windows, Unix or Linux. MySQL is almost same as Oracle server,

which has same available for every system. Trivedi G. (2010) also mentioned that DB2 database is also available for every operating system like Windows, Unix and Linux.

2.7.5 Backup and Recovery

Shekhar R. (2011) said that Oracle provides different type backup facilities such as cold backup, hot backup, export, import and data pump. Oracle offers most popular backup utility called Recovery Manager (RMAN) while MySQL has mysqldump and mysqlhotcopy backup utilities but there is no utility like RMAN in MySQL. As said by Ebbers M. et al. (2009), DB2 has a COPY utility to recover data and there is MERGECOPY utility to merge incremental copies with a full copy. RECOVER utility in DB2 can recover back to an image copy for a point-in-time recovery.

2.7.6 Storage

As said by Shekhar R. (2011), MySQL doesn't have Table space, Role management, snapshots, synonym and packages compare to Oracle. In contrast, Oracle has Table space, Role management, snapshots, synonym and packages. On the other hand, Ebbers M. et al. (2009) mentioned that DB2 has a storage group consists of a set of volumes on disks (DASD) that hold the data sets in which tables and indexes are actually stored. DB2 also has view, Table space and Index space.

2.8 Computers

According to Roper M. and Millar L. (1999), a computer is a programmable machine. There are several different types of computer such as Mainframe computers, Mini-computers, workstations and Personal computers. Here, the different between Personal computers and Mainframe computers will be reviews regarding its definition and functions, components and operating system.

2.8.1 Definition and functions

According to Ebbers M. et al. (2009), mainframe means computers that can support thousand of applications and input/output devices to simultaneously server thousands of users. Vigil J. and Price J. (2002) said that mainframe is used connect multiple users for large organization while personal computers are generally used for a single users. Roper M. and Millar L. (1999) also noted that personal computers (PCs), also called microcomputers, are the most popular type of computer in use nowadays.

2.8.2 Components

Vigil J. and Price J. (2002) said that both mainframe and personal computer have processors, storage, memory, operating systems and displays. Roper M. and Millar L. (1999) also noted that computer are made up of two parts which are hardware and software. Hardware components are central processing unit (CPU), memory, storage device, input devices, output devices, random access memory (RAM), storage, optical disk, hard drive and magnetic tape.